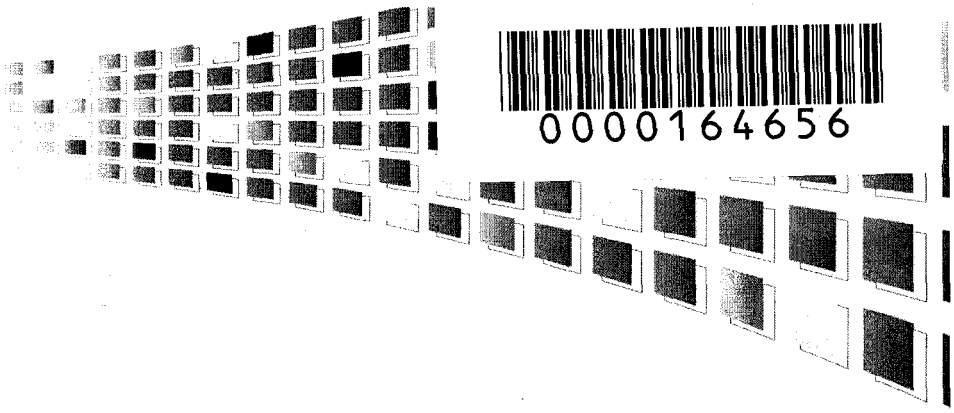
MARASHLIAN & DONAHUE, LLC
THE COMMLAW GROUP



ORIGINAL

September 1, 2015

Via Overnight Courier

Docket Control
Arizona Corporation Commission
1200 West Washington Street
Phoenix, AZ 85007

RE: Revised Response to STF 1.9 in Staff's First Set of Data Requests to Mobilitie, LLC (Docket No. T-20913A-15-0191)

Dear Sir or Madam:

Enclosed for filing please find an original and thirteen (13) copies of Mobilitie, LLC's Revised Response to STF 1.9 in Staff's First Set of Data Requests under the above referenced docket. A copy of this filing has also been served via email to Mr. Matthew Connolly at mconnolly@azcc.gov. As Staff requested further clarification to the response originally provided to STF 1.9, we are providing this clarification in the attached revised response. We ask that this replace the response to STF 1.9 filed on August 19, 2015.

The revised response to STF 1.9 is jointly provided by undersigned counsel, Jon Buck, Director of Network Deployment and Ethan Rogers, Corporate Counsel. The latter two individuals are employees of Mobilitie, LLC with business address at 2220 University Drive, Newport Beach, CA 92660.

If you have any questions or concerns regarding this filing please do not hesitate to contact me at vmp@commlawgroup.com or (703) 714-1309.

Respectfully submitted,

Vineetha Pillai
Counsel for Mobilitie, LLC

cc: Matthew Connolly, Utilities Division (electronic delivery)

1420 Spring Hill Road, Suite 401
McLean, Virginia 22102
P 703.714.1300
F 703.563.6222
W www.commlawgroup.com
E mail@commlawgroup.com

REVISED RESPONSE TO STF 1.9 IN STAFF'S FIRST SET OF DATA REQUESTS TO
MOBILITIE, LLC. ("MOBILITIE")
DOCKET NO. T-20913A-15-0191
September 1, 2015

STF 1.9 What steps and precautions has Mobilitie taken in order to ensure the security of its networks and equipment? If none exist, what protections does the company have planned?

Response: Mobilitie's mobile and wireless infrastructure utilizes software for network monitoring, reporting and user device authentication. Mobilitie ensures that the software is secure and allows for ease of connectivity. Mobilitie utilizes network security software solutions that allow for secure connection on all portions of the network.

With respect to the structures/antennas and pole attachments Mobilitie is engaged in the construction of, they comply with all jurisdictional industry standards when securing the structures on rights-of-way. In addition, they retain only licensed contractors, and are compliant with the National Engineering Safety Code's standards for construction. Further, the municipalities in which they construct are indemnified if anything should go wrong with respect to securing of the equipment itself

Mobilitie complies with applicable law and Industry Data Safeguards concerning end user data and other confidential information. "Industry Data Safeguards" means those data security practices, procedures and safeguards typically implemented by US corporations and include among other things:

(a) ensuring the physical security of servers and any equipment by which data may be accessed, using secure data centers that utilize redundant power and cooling, and fire suppression systems;

(b) restricting data center access to authorized individuals only and ensuring that all access is monitored and recorded for audit purposes;

(c) employing redundant backup systems and disaster mitigation and failover plans;

(d) maintaining physical safeguards of data;

(e) using up to date firewalls and intrusion detection systems and scanning systems with security vulnerability scanning software at regular intervals;

(g) encryption or compensating controls to protect extremely sensitive data such as credit card information or any data required by applicable legal requirements;

(i) enforcing security standards and access controls for and by its employees and contractors, limiting access to confidential information to persons with a need to know;

(j) installing antivirus software on all production Windows-based servers and desktops/laptops that is configured to automatically download up-to-date virus signatures from a trusted third party source; and

(k) implementing other industry standard security systems, procedures and protocols.